(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
6 octobre 2005 (06.10.2005)

PCT

(10) Numéro de publication internationale
WO 2005/093993 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/EP2005/050729

(22) Date de dépôt international :
18 février 2005 (18.02.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0402006 27 février 2004 (27.02.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne Parc, d'activité de Gémenos, F-13420 GEMENOS (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **NACCACHE, David** [FR/FR]; 52 rue Letort, F-75018 PARIS (FR).

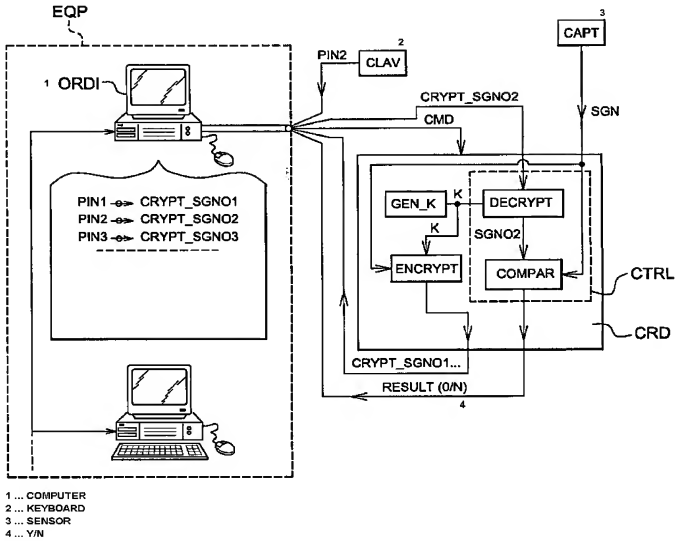
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH,

[Suite sur la page suivante]

(54) Title: IMPROVED METHOD, AUTHENTICATION MEDIUM AND DEVICE FOR SECURING ACCESS TO A PIECE OF EQUIPMENT

(54) Titre : PROCEDE, SUPPORT D'AUTHENTIFICATION, ET DISPOSITIF PERFECTIONNES POUR LA SECURISATION D'UN ACCES A UN EQUIPEMENT



(57) **Abstract:** The invention relates to a device for securing access to a piece of equipment (EQP), comprising an authentication medium (CRD) which uses a reference datum and control means (CTRL) which can be used to verify the consistency between the reference datum and a biometric signature (SGN) obtained from a party requesting access. According to the invention, the reference datum comprises an encrypted version (CRYPT_SGN02) of an authentic biometric signature (SGN02) attributed to the party requesting access, and the aforementioned data consistency is verified by comparing (COMPAR) the biometric signature (SGN) obtained from a party requesting access to an authentic biometric signature (SGN02) resulting from decryption of the encrypted version (CRYPT SGN02) of said signature using a secret key (K).

[Suite sur la page suivante]

WO 2005/093993 A1

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne notamment un dispositif de sécurisation d'un accès à un équipement (EQP), comprenant un support d'authentification (CRD) utilisant: une donnée de référence et incluant des moyens de contrôle (CTRL) permettant de vérifier la cohérence entre la donnée de référence et une signature biométrique (SGN) obtenue d'un demandeur d'accès. Selon l'invention, la donnée de référence est constituée par une version cryptée (CRYPT_SGN02) d'une signature biométrique authentique (SGN02) supposée attribuée au demandeur d'accès, et la cohérence précédemment mentionnée est vérifiée en comparant (COMPAR) la signature biométrique (SGN) obtenue d'un demandeur d'accès à une signature biométrique authentique (SGN02) résultant d'un décryptage, au moyen d'une clef secrète (K), de la version cryptée (CRYPT SGN02) de cette signature.

PROCEDE, SUPPORT D'AUTHENTIFICATION, ET DISPOSITIF PERFECTIONNES POUR LA SECURISATION D'UN ACCES A UN EQUIPEMENT.

L'invention concerne, de façon générale, les techniques biométriques d'authentification visant à contrôler l'accès à des informations sensibles.

Plus précisément, l'invention concerne, selon un premier de ses aspects, un procédé de sécurisation d'un accès à un équipement, ce procédé comprenant au moins : une opération d'attribution consistant à fournir une donnée de référence à un support d'authentification; une opération d'acquisition consistant à obtenir, à chaque requête d'accès formulée par un demandeur d'accès à l'équipement, une signature biométrique de ce demandeur d'accès; et une étape de vérification consistant à vérifier, en utilisant la donnée de référence, l'authenticité de la signature biométrique obtenue du demandeur d'accès.

L'authentification de personnes par signature biométrique, telle par exemple qu'une empreinte digitale ou l'image de l'iris d'un œil, présente intrinsèquement une sélectivité très élevée, mais pose des problèmes spécifiques que ne pose pas l'authentification au moyen d'un code numérique personnel saisi par la personne sollicitant un accès à un équipement protéger.

En effet, dans le cas typique où l'équipement protégé comprend un ordinateur, l'authentification par code est facilement mise en œuvre en cachant le code numérique authentique fractionné dans la mémoire de l'ordinateur, en

le recomposant à chaque requête d'accès, et en comparant à l'identique le code authentique recomposé au code proposé par un demandeur d'accès.

Or, l'authentification par signature biométrique ne peut pas être mise en œuvre de la même façon dans la mesure où seules, dans ce dernier cas, peuvent être repérées des ressemblances ou des dissemblances entre une signature biométrique authentique et une signature biométrique proposée par un demandeur d'accès.

Cette singularité de l'authentification par signature biométrique oblige en pratique à mémoriser les signatures biométriques authentiques en clair sur le disque dur de l'ordinateur, de sorte qu'un pirate parvenant à accéder une seule fois à ce disque peut en retirer l'information qui lui permettra d'y accéder facilement autant de fois qu'il le souhaite par la suite en déconnectant le capteur biométrique et en injectant les données directement dans la machine cible.

L'invention a principalement pour but de proposer une solution à ce problème.

A cette fin, le procédé de l'invention, par ailleurs conforme à la définition générique qu'en donne le préambule ci-dessus, est essentiellement caractérisé en ce qu'il comporte une étape préalable de cryptage au cours de laquelle est élaborée une version cryptée d'au moins une signature biométrique authentique appartenant à au moins une personne autorisée à accéder à l'équipement, en ce que l'étape de vérification comprend une opération de décryptage mise en œuvre dans le support d'authentification

et consistant à décrypter, au moyen d'une clef secrète, la version cryptée d'une signature biométrique authentique fournie à ce support d'authentification en tant que donnée de référence lors de la requête d'accès, et en ce que l'étape de vérification comprend une opération de comparaison mise en œuvre en comparant secrètement la signature biométrique obtenue du demandeur d'accès lors de la requête d'accès à la signature biométrique authentique issue du décryptage.

Un support d'authentification pour la mise en œuvre de ce procédé prend par exemple la forme d'une carte électronique comportant au moins un module de décryptage utilisant une clef secrète, ce support pouvant en outre comporter un module de comparaison ainsi, éventuellement, qu'un module de cryptage.

L'invention concerne également un dispositif de sécurisation d'un accès à un équipement, comprenant : un support d'authentification auquel est fournie une donnée de référence; un capteur obtenant, à chaque requête d'accès formulée par un demandeur d'accès à l'équipement, une signature biométrique de ce demandeur d'accès; et des moyens de contrôle inclus dans le support d'authentification et autorisant sélectivement le demandeur d'accès à accéder à l'équipement en fonction du résultat d'une vérification de l'authenticité de la signature biométrique du demandeur d'accès au moyen de la donnée de référence, ce dispositif étant caractérisé en ce que les moyens de contrôle comprennent un module de décryptage et un module de comparaison, en ce que la donnée de référence fournie au support d'authentification est constituée par une version cryptée d'une signature biométrique authentique

supposée attribuée au demandeur d'accès, en ce que le module de décryptage utilise une clef secrète au moyen de laquelle il reconstitue secrètement, à chaque requête d'accès, la signature biométrique authentique à partir de sa version cryptée, et en ce que le module de comparaison compare secrètement la signature biométrique obtenue du demandeur d'accès à la signature biométrique authentique reconstituée, et fournit un résultat de comparaison constituant le résultat de la vérification.

Outre le support d'authentification, par exemple constituée par une carte, amovible ou non, dotée d'une mémoire non lisible de l'extérieur et dans laquelle est stockée la clef secrète, le dispositif de l'invention peut aussi comprendre un ou plusieurs ordinateurs constituant une partie au moins de l'équipement dont l'accès est sécurisé.

Dans ce cas, l'ordinateur ou l'un d'entre eux peut contenir en mémoire une pluralité de codes d'identification personnels attribués à une pluralité correspondante de personnes autorisées à accéder à l'équipement et associés à une pluralité correspondante de signatures biométriques authentiques cryptées de ces personnes autorisées, cet ordinateur pouvant alors délivrer au support d'identification, lors d'une requête d'accès, la signature biométrique authentique cryptée correspondant au code d'identification fourni par le demandeur d'accès.

Un même support d'authentification peut ainsi offrir à plusieurs personnes un accès sécurisé à l'ordinateur.

Le dispositif de l'invention peut inclure un module de cryptage propre à délivrer, en réponse à une commande de

cryptage, une version cryptée d'une signature biométrique authentique fournie en clair par le capteur.

Dans le cas où la clef secrète est une clef privée à laquelle correspond une clef publique, le module de cryptage peut avantageusement être inclus dans l'ordinateur et utiliser la clef publique du support d'authentification.

D'autres caractéristiques et avantages de l'invention ressortiront clairement de la description qui en est faite ci-après, à titre indicatif et nullement limitatif, en référence aux dessins annexés, dans lesquels :

- la figure 1 est un schéma représentant un premier mode de réalisation possible de l'invention; et

- la figure 2 est un schéma représentant un second mode de réalisation possible de l'invention.

Sur ces figures, l'équipement EQP dont l'accès est sécurisé est représenté comme incluant un ordinateur ORDI, et cet ordinateur est lui-même schématiquement représenté comme relié à un clavier CLAV, à un capteur CAPT, et à un support d'authentification CRD dont il peut partiellement contrôler le fonctionnement par une commande CMD, l'homme du métier étant en mesure de mettre en œuvre tous les moyens concrets connus, et notamment les lecteurs de cartes, pour établir les liaisons et interactions fonctionnelles représentées.

Comme annoncé précédemment, l'invention permet de sécuriser l'accès à un équipement EQP au moyen d'une authentification biométrique des personnes sollicitant l'accès à cet équipement.

Pour ce faire, l'invention utilise, de façon connue en soi, un support d'authentification CRD prenant de préférence la forme d'une carte à puce électronique, dotée d'une mémoire non lisible de l'extérieur.

A chaque requête d'accès formulée par un demandeur d'accès à l'équipement EPQ, une signature biométrique SGN du demandeur d'accès, par exemple son empreinte digitale, est détectée par le capteur CAPT et transmise au support d'authentification CRD.

Ce support d'authentification CRD vérifie alors, grâce à des moyens de contrôle CTRL dont il est doté et en utilisant une donnée de référence chiffrée stockée sur EQP ou ORDI et qui lui est fournie par EQP ou ORDI, l'authenticité de la signature biométrique SGN obtenue du demandeur d'accès, et délivre un résultat de comparaison RESULT qui déclenche ou non une autorisation d'accès à l'équipement EPQ.

Selon l'invention, la donnée de référence utilisée à chaque requête d'accès par le support d'authentification CRD est constituée par une version cryptée, telle par exemple que CRYPT_SGN02, d'une signature biométrique authentique, telle par exemple que SGN02, appartenant une personne autorisée à accéder à l'équipement.

Le procédé de l'invention comporte donc une étape préalable d'enregistrement des personnes autorisées à accéder à l'équipement EQP, au cours de laquelle est élaborée chacune des versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03

des signatures biométriques authentiques SGN01, SGN02, SGN03 de ces différentes personnes.

Dans le mode de réalisation de la figure 1, ce cryptage préalable est effectué dans la carte CRD, à réception d'un signal de commande CMD approprié, par un module de cryptage ENCRYPT utilisant une clef secrète K délivrée par un générateur de clef GEN_K interne à la carte CRD, ce cryptage étant réalisé sur les signatures biométriques authentiques SGN01, SGN02, SGN03 reçues du capteur CAPT et appartenant aux personnes physiquement identifiées comme étant autorisées à accéder à cet équipement.

Les versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03 des différentes signatures biométriques authentiques SGN01, SGN02, SGN03 sont ensuite transférées par la carte CRD, à réception d'un signal de commande CMD approprié, vers le disque dur de l'ordinateur ORDI où elles sont stockées.

Le système de cryptage utilisé est alors par exemple conforme à la norme de cryptage avancée connue de l'homme de métier sous son acronyme anglais AES (pour "Advanced Encryption Standard").

Les moyens de contrôle CTRL prévus dans la carte CRD comprennent un module de décryptage DECRYPT et un module de comparaison COMPAR.

Ainsi, pour procéder à l'authentification d'une signature biométrique SGN soumise par un demandeur d'accès, la carte CRD opère en deux temps.

Tout d'abord, le module de décryptage DECRYPT de cette carte décrypte, au moyen de la clef secrète K interne à la carte CRD, la version cryptée CRYPT_SGN02 de la signature biométrique authentique SGN02 qui est supposée être celle du demandeur d'accès, et que l'ordinateur ORDI fournit à la carte CRD en tant que donnée de référence lors de la requête d'accès.

Puis, le module de comparaison COMPAR de la carte CRD compare secrètement la signature biométrique SGN, obtenue du demandeur d'accès par l'intermédiaire du capteur CAPT lors de la requête d'accès, à la signature biométrique authentique SGN02 reconstituée par le module de décryptage à partir de sa version cryptée CRYPT_SGN02.

Enfin, le module de comparaison COMPAR fournit à l'ordinateur ORDI un résultat de comparaison RESULT, qui constitue le résultat de la vérification effectuée, et qui contient pour seule information l'indication du caractère authentique ou non de la signature biométrique SGN obtenue du demandeur d'accès.

Dans le mode de réalisation illustré à la figure 2, le générateur de clef GEN_K interne à la carte CRD fournit d'une part, en tant que clef secrète interne à cette carte, une clef privée K0, et d'autre part une clef publique K1 correspondant à cette clef privée K0 et qui peut être fournie au monde extérieur, notamment à l'ordinateur ORDI.

Dans ce mode de réalisation, les versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03 sont obtenues en cryptant, au moyen de la clef publique K1, les différentes signatures biométriques authentiques SGN01, SGN02, SGN03,

et ces signatures biométriques authentiques SGN01, SGN02, SGN03 sont reconstruites dans la carte CRD à partir de leurs versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03 au moyen d'un décryptage utilisant la clef privée K0.

Dans ces conditions, comme illustré sur la figure 2, la clef publique K1 peut être stockée dans la mémoire de masse de l'ordinateur ORDI et le module de cryptage ENCRYPT_K1 peut lui-même être prévu dans cet ordinateur, la caractéristique importante étant, comme dans le premier mode de réalisation, que les signatures biométriques authentiques SGN01, SGN02, SGN03 ne soient pas en permanence mémorisées en clair dans l'ordinateur ORDI.

Contrairement à la technique traditionnelle, dans laquelle le support d'authentification CRD contient la donnée de référence constituée par une signature biométrique en clair, l'invention prévoit que ce support ne contienne qu'une clef secrète, c'est-à-dire une information dépersonnalisée.

Dans ces conditions, l'invention ouvre la possibilité qu'un même support d'authentification CRD offre à plusieurs personnes un accès sécurisé à l'ordinateur ORDI.

La seule contrainte est que la signature biométrique de chaque demandeur d'accès puisse effectivement être comparée à une signature biométrique authentique supposée a priori attribuée à ce demandeur.

Si le nombre de personnes autorisées à accéder à l'équipement EQP est faible, il est imaginable qu'à chaque

requête d'accès l'ordinateur ORDI fournisse à la carte CRD les versions cryptées CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03 des signatures biométriques authentiques SGN01, SGN02, SGN03 de toutes les personnes autorisées à accéder à l'équipement, et que l'accès soit autorisé dès lors que l'une des signatures authentiques décryptées correspond à la signature SGN obtenue du demandeur d'accès.

Si en revanche le nombre de personnes autorisées à accéder à l'équipement EQP est relativement élevé, il peut être utile de prévoir que chaque demandeur d'accès s'identifie a priori par un code personnel tel que PIN1, PIN2, PIN3, ce code n'ayant cependant pas besoin d'être lui-même confidentiel puisqu'il ne sert qu'à sélectionner la version cryptée de signature biométrique invoquée a priori par le demandeur d'accès lors de sa requête d'accès, et non à faire droit à cette requête.

Concrètement, chaque personne autorisée à accéder à l'équipement EQP peut être identifiée, lors de l'étape préalable d'enregistrement, par un tel code personnel PIN1, PIN2, PIN3, et le code personnel de chaque personne peut être mémorisé dans l'ordinateur ORDI de manière à être mis en correspondance avec la signature biométrique authentique cryptée de cette personne.

Lors d'une requête d'accès, le demandeur d'accès peut ainsi s'identifier en composant son code personnel sur le clavier CLAV, l'ordinateur ORDI délivrant au support d'identification CRD la signature biométrique authentique cryptée, par exemple CRYPT_SGN02, correspondant au code d'identification fourni par le demandeur d'accès, par exemple PIN2.

REVENDICATIONS

1. Procédé de sécurisation d'un accès à un équipement (EQP), ce procédé comprenant au moins : une opération d'attribution consistant à fournir une donnée de référence (CRYPT_SGN02) à un support d'authentification (CRD); une opération d'acquisition consistant à obtenir, à chaque requête d'accès formulée par un demandeur d'accès à l'équipement, une signature biométrique (SGN) de ce demandeur d'accès; et une étape de vérification consistant à vérifier, en utilisant la donnée de référence (CRYPT_SGN02), l'authenticité de la signature biométrique (SGN) obtenue du demandeur d'accès, caractérisé en ce qu'il comporte une étape préalable de cryptage au cours de laquelle est élaborée une version cryptée (CRYPT_SGN02) d'au moins une signature biométrique authentique (SGN02) appartenant à au moins une personne autorisée à accéder à l'équipement, en ce que l'étape de vérification comprend une opération de décryptage mise en œuvre dans le support d'authentification (CRD) et consistant à décrypter, au moyen d'une clef secrète (K, K0), la version cryptée (CRYPT_SGN02) d'une signature biométrique authentique (SGN02) fournie à ce support d'authentification (CRD) en tant que donnée de référence lors de la requête d'accès, et en ce que l'étape de vérification comprend une opération de comparaison mise en œuvre en comparant secrètement la signature biométrique (SGN) obtenue du demandeur d'accès lors de la requête d'accès à la signature biométrique authentique (SGN02) issue du décryptage.

2. Support d'authentification pour la mise en œuvre du procédé suivant la revendication 1, caractérisé en ce qu'il prend la forme d'une carte électronique comportant au moins

un module de décryptage (DECRYPT) utilisant une clef secrète (K, K0).

3. Support d'authentification suivant la revendication 2, caractérisé en ce qu'il comporte en outre un module de comparaison (COMPAR).

4. Support d'authentification suivant la revendication 2 ou 3, caractérisé en ce qu'il comporte en outre un module de cryptage (ENCRYPT).

5. Dispositif de sécurisation d'un accès à un équipement, ce dispositif comprenant : un support d'authentification (CRD) auquel est fournie une donnée de référence (CRYPT_SGN02); un capteur (CAPT) obtenant, à chaque requête d'accès formulée par un demandeur d'accès à l'équipement, une signature biométrique (SGN) de ce demandeur d'accès; et des moyens de contrôle (CTRL) inclus dans le support d'authentification (CRD) et autorisant sélectivement le demandeur d'accès à accéder à l'équipement (EQP) en fonction du résultat d'une vérification de l'authenticité de la signature biométrique du demandeur d'accès au moyen de la donnée de référence (CRYPT_SGN02), caractérisé en ce que les moyens de contrôle (CTRL) comprennent un module de décryptage (DECRYPT) et un module de comparaison (COMPAR), en ce que la donnée de référence (CRYPT_SGN02) fournie au support d'authentification (CRD) est constituée par une version cryptée d'une signature biométrique authentique (SGN02) supposée attribuée au demandeur d'accès, en ce que le module de décryptage (DECRYPT) utilise une clef secrète (K, K0) au moyen de laquelle il reconstitue secrètement, à chaque requête d'accès, la signature biométrique authentique (SGN02) à partir de sa version cryptée

(CRYPT_SGN02), et en ce que le module de comparaison (COMPAR) compare secrètement la signature biométrique (SGN) obtenue du demandeur d'accès à la signature biométrique authentique (SGN02) reconstituée, et fournit un résultat de comparaison (RESULT) constituant le résultat de la vérification.

6. Dispositif de sécurisation suivant la revendication 5, caractérisé en ce que le support d'authentification (CRD) est une carte, amovible ou non-amovible, dotée d'une mémoire non lisible de l'extérieur et dans laquelle est stockée la clef secrète (K, K0).

7. Dispositif de sécurisation suivant l'une quelconque des revendications 5 et 6, caractérisé en ce qu'il comprend au moins un ordinateur (ORDI) constituant une partie au moins de l'équipement (EQP) dont l'accès est sécurisé.

8. Dispositif de sécurisation suivant la revendication 7, caractérisé en ce que l'ordinateur (ORDI) contient en mémoire une pluralité de codes d'identification personnels (PIN1, PIN2, PIN3) attribués à une pluralité correspondante de personnes autorisées à accéder à l'équipement et associés à une pluralité correspondante de signatures biométriques authentiques cryptées (CRYPT_SGN01, CRYPT_SGN02, CRYPT_SGN03) de ces personnes autorisées, et en ce que l'ordinateur (ORDI) délivre au support d'identification (CRD), lors d'une requête d'accès, la signature biométrique authentique cryptée (CRYPT_SGN02) correspondant au code d'identification (PIN2) fourni par le demandeur d'accès, ce dont il résulte qu'un même support d'authentification (CRD) offre à plusieurs personnes un accès sécurisé à l'ordinateur (ORDI).

9. Dispositif de sécurisation suivant l'une quelconque des revendications 5 à 8, caractérisé en ce qu'il comporte un module de cryptage (ENCRYPT, ENCRYPT_K1) propre à délivrer, en réponse à une commande de cryptage, une version cryptée d'une signature biométrique authentique fournie en clair par le capteur (CAPT).

10. Dispositif de sécurisation suivant la revendication 9, caractérisé en ce que la clef secrète (K0) est une clef privée à laquelle correspond une clef publique (K1), et en ce que le module de cryptage (ENCRYPT_K1) est inclus dans l'ordinateur (ORDI) et utilise la clef publique (K1).

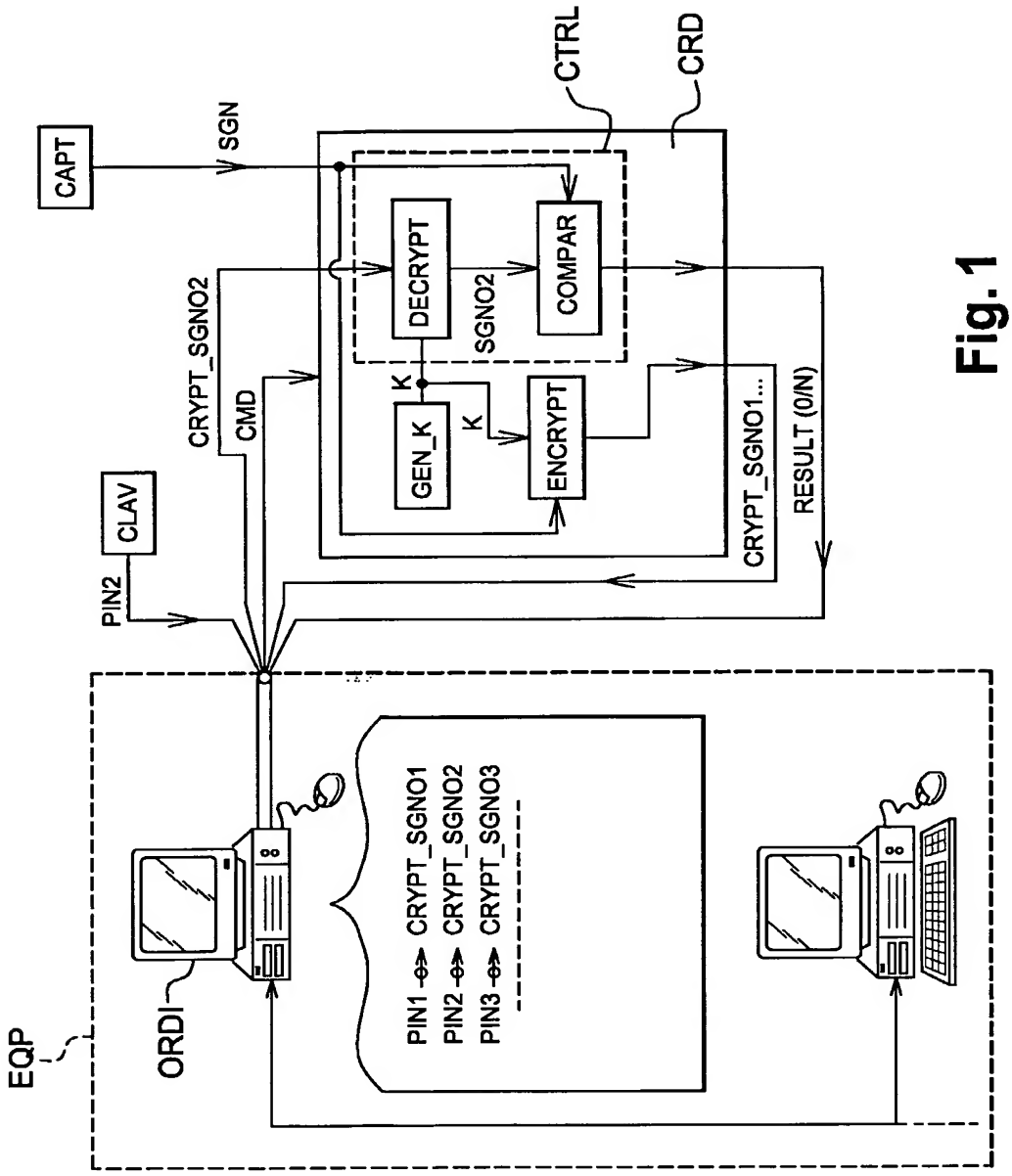

CAPT
SGN
CTRL
CRD
DECRYPT
COMPAR
SGNO2
CRYPT_SGNO2
CMD
K
GEN_K
K
ENCRYPT
CRYPT_SGNO1...
RESULT (0/N)
CLAV
PIN2
EQP
ORDI
PIN1 CRYPT_SGNO1
PIN2 CRYPT_SGNO2
PIN3 CRYPT_SGNO3

Fig. 1

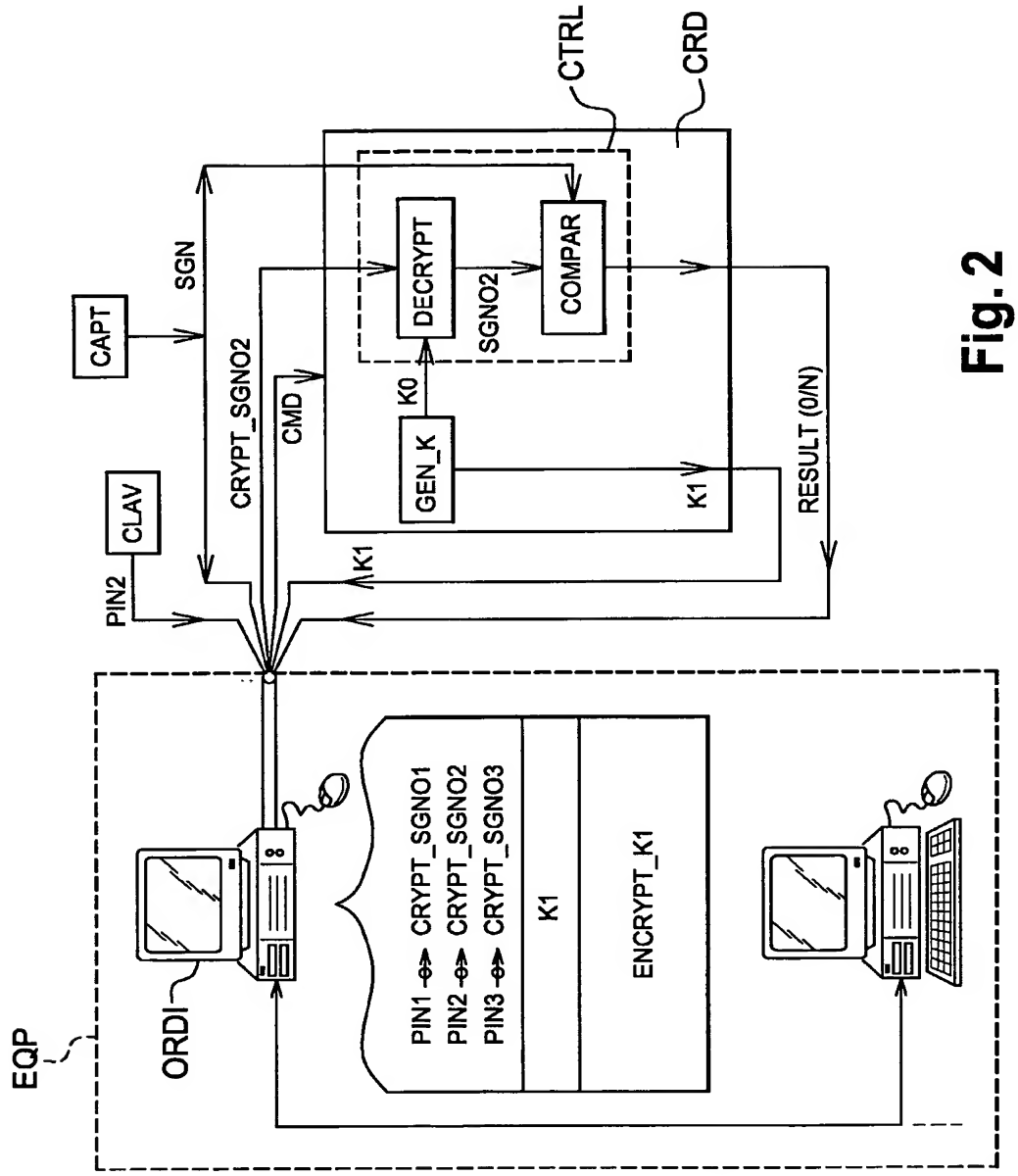

CTRL
CRD
SGN
CAPT
DECRYPT
COMPAR
SGNO2
K0
CRYPT_SGNO2
CMD
GEN_K
K1
RESULT (0/N)
CLAV
K1
PIN2
EQP
ORDI
PIN1 → CRYPT_SGNO1
PIN2 → CRYPT_SGNO2
PIN3 → CRYPT_SGNO3
K1
ENCRYPT_K1

Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/050729

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G07C G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/069361 A1 (ISHIBASHI YOSHIHITO ET AL) 6 June 2002 (2002-06-06) paragraph '0001! - paragraph '0016!	1-7,9,10
Y	paragraph '0355! - paragraph '0357! figure 27	8
X	EP 1 265 121 A (SYSTEMNEEDS INC) 11 December 2002 (2002-12-11) paragraph '0001! - paragraph '0013! paragraph '0049! - paragraph '0051! figure 2	1-7,9,10
Y	US 6 317 834 B1 (HALEVI SHAI ET AL) 13 November 2001 (2001-11-13) column 1, line 5 - column 2, line 5 column 6, line 30 - line 39 column 6, line 56 - column 7, line 50	8

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 April 2005	29/04/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Liebhardt, I

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/088782 A1 (FORREST SIMON J) 8 May 2003 (2003-05-08) paragraph '0001! - paragraph '0003! paragraph '0038! - paragraph '0044! figure 1 -----	8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/050729

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002069361 A1	06-06-2002	JP 2002169465 A	14-06-2002
EP 1265121 A	11-12-2002	JP 2003085149 A	20-03-2003
		CA 2389632 A1	07-12-2002
		EP 1265121 A2	11-12-2002
		US 2002188855 A1	12-12-2002
US 6317834 B1	13-11-2001	NONE	
US 2003088782 A1	08-05-2003	GB 2381916 A	14-05-2003
		EP 1449322 A2	25-08-2004
		WO 03041324 A2	15-05-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2005/050729

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G07C G07F G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X Y	US 2002/069361 A1 (ISHIBASHI YOSHIHITO ET AL) 6 juin 2002 (2002-06-06) alinéa '0001! - alinéa '0016! alinéa '0355! - alinéa '0357! figure 27 -----	1-7,9,10 8
X	EP 1 265 121 A (SYSTEMNEEDS INC) 11 décembre 2002 (2002-12-11) alinéa '0001! - alinéa '0013! alinéa '0049! - alinéa '0051! figure 2 -----	1-7,9,10
Y	US 6 317 834 B1 (HALEVI SHAI ET AL) 13 novembre 2001 (2001-11-13) colonne 1, ligne 5 - colonne 2, ligne 5 colonne 6, ligne 30 - ligne 39 colonne 6, ligne 56 - colonne 7, ligne 50 ----- -/--	8

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
21 avril 2005	29/04/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Liebhardt, I

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/EP2005/050729

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 2003/088782 A1 (FORREST SIMON J) 8 mai 2003 (2003-05-08) alinéa '0001! - alinéa '0003! alinéa '0038! - alinéa '0044! figure 1 -----	8

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/EP2005/050729

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 2002069361	A1	06-06-2002	JP	2002169465 A	14-06-2002
EP 1265121	A	11-12-2002	JP	2003085149 A	20-03-2003
			CA	2389632 A1	07-12-2002
			EP	1265121 A2	11-12-2002
			US	2002188855 A1	12-12-2002
US 6317834	B1	13-11-2001	AUCUN		
US 2003088782	A1	08-05-2003	GB	2381916 A	14-05-2003
			EP	1449322 A2	25-08-2004
			WO	03041324 A2	15-05-2003